THE CLAIMS

Claims 1-42 are pending in the instant application.

Listing of claims:

1. (Previously presented) A method for multiple encryption in a multi-band multi-protocol hybrid wired/wireless network, the method comprising:

receiving on a first PHY channel of an access point, a request for initiation of a communication session from an originating access device;

authenticating said communication session by authenticating said originating access device using a second PHY channel; and

hosting said communication session over a third PHY channel, said third PHY channel established between said access point and said originating access device.

2. (Previously presented) The method according to claim 1, comprising generating at least one encryption/decryption key for use during said communication session.

3. (Previously presented) The method according to claim 2, wherein said authenticating comprises requesting authentication information from an authentication server.

4. (Previously presented) The method according to claim 3, wherein said authenticating comprises delivering at least a portion of said authentication information received from said authentication server to said originating access device via said second PHY channel.

5. (Previously presented) The method according to claim 4, comprising delivering said at least one encryption/decryption key to said originating access device via one of said first PHY channel or said second PHY channel.

6. (Previously presented) The method according to claim 1, comprising receiving an identification of said originating access device by said access point.

7. (Previously presented) The method according to claim 6, wherein said identity of said originating access device is one or more of a WEP key, a MAC address, and/or an IP address.

8. (Previously presented) The method according to claim 1, comprising acknowledging said received request on said first PHY channel.

9. (Previously presented) The method according to claim 1, comprising determining a type of traffic generated by said originating access device on said first PHY channel.

10. (Previously presented) The method according to claim 9, comprising generating at least one encryption/decryption key dependent on said determined traffic type.

11. (Previously presented) The method according to claim 10, comprising distributing said generated at least one encryption/decryption key via one or both of said second PHY channel and/or said third PHY channel.

12. (Previously presented) The method according to claim 1, comprising establishing at least one virtual channel between said originating access device and a terminating access device.

13. (Previously presented) The method according to claim 12, comprises tunneling information between said originating access device and said terminating access device.

14. (Previously presented) The method according to claim 12, comprising establishing at least a portion of said at least one virtual channel over at least a portion of one of said first PHY channel, said second PHY channel or said third PHY channel.

15. (Previously presented) A machine-readable storage, having stored thereon, a computer program having at least one code section for providing

multiple encryption in a multi-band multi-protocol hybrid wired/wireless network, the at least one code section executable by a machine for causing the machine to perform the steps comprising:

receiving on a first PHY channel of an access point, a request for initiation of a communication session from an originating access device;

authenticating said communication session by authenticating said originating access device using a second PHY channel; and

hosting said communication session over a third PHY channel, said third PHY channel established between said access point and said originating access device.

16. (Previously presented) The machine-readable storage according to claim 15, comprising code for generating at least one encryption/decryption key for use during said communication session.

17. (Previously presented) The machine-readable storage according to claim 16, wherein authenticating code comprises code for requesting authentication information from an authentication server.

18. (Previously presented) The machine-readable storage according to claim 17, comprising code for delivering at least a portion of said authentication information received from said authentication server to said originating access device via said second PHY channel.

19. (Previously presented) The machine-readable storage according to claim 18, comprising code for delivering said at least one encryption/decryption key to said originating access device via one of said first PHY channel or said second PHY channel.

20. (Previously presented) The machine-readable storage according to claim 15, comprising code for receiving an identification of said originating access device by said access point.

21. (Previously presented) The machine-readable storage according to claim 20, wherein said identity of said originating access device is one or more of a WEP key, a MAC address, and/or an IP address.

22. (Previously presented) The machine-readable storage according to claim 15, comprising code for acknowledging said received request on said first PHY channel.

23. (Previously presented) The machine-readable storage according to claim 15, comprising code for determining a type of traffic generated by said originating access device on said first PHY channel.

24. (Previously presented) The machine-readable storage according to claim 23, comprising code for generating at least one encryption/decryption key dependent on said determined traffic type.

25. (Previously presented) The machine-readable storage according to claim 24, comprising code for distributing said generated at least one encryption/decryption key via one or both of said second PHY channel and/or said third PHY channel.

26. (Previously presented) The machine-readable storage according to claim 15, comprising code for establishing at least one virtual channel between said originating access device and a terminating access device.

27. (Previously presented) The machine-readable storage according to claim 26, comprises code for tunneling information between said originating access device and said terminating access device.

28. (Previously presented) The machine-readable storage according to claim 26, comprising code for establishing at least a portion of said at least one virtual channel over at least a portion of one of said first PHY channel, said second PHY channel or said third PHY channel.

29. (Previously presented) A system for multiple encryption in a multi-band multi-protocol hybrid wired/wireless network, the system comprising:

at least one receiver of an access point adapted to receive on a first PHY channel, a request for initiation of a communication session from an originating access device;

at least one authenticator adapted to authenticate said communication session by authenticating said originating access device using a second PHY channel; and

a third PHY channel being adapted to facilitate hosting of said communication session, said third PHY channel established between said access point and said originating access device.

30. (Original) The system according to claim 29, wherein said at least one authenticator is adapted to generate at least one encryption/decryption key for use during said communication session.

31. (Original) The system according to claim 30, wherein said at least one authenticator is adapted to receive requests for authentication information.

32. (Original) The system according to claim 31, wherein said authenticator is adapted to deliver at least a portion of said authentication information received from said authentication server to said originating access device via said second PHY channel.

33. (Previously presented) The system according to claim 32, wherein said at least one authenticator is adapted to deliver said at least one encryption/decryption key to said originating access device via one of said first PHY channel or said second PHY channel.

34. (Original) The system according to claim 29, wherein said at least one receiver is adapted to receive an identification of said originating access device by said access point.

35. (Previously presented) The system according to claim 34, wherein said identity of said originating access device is one or more of a WEP key, a MAC address, and/or an IP address.

36. (Original) The system according to claim 29, wherein said at least one receiver is adapted to acknowledge said received request on said first PHY channel.

37. (Original) The system according to claim 29, wherein said at least one authenticator is adapted to determine a type of traffic generated by said originating access device on said first PHY channel.

38. (Original) The system according to claim 37, wherein said at least one authenticator is adapted to generate at least one encryption/decryption key dependent on said determined traffic type.

39. (Previously presented) The system according to claim 38, wherein said at least one authenticator is adapted to distribute said generated at least one

encryption/decryption key via one or both of said second PHY channel and/or said third PHY channel.

40. (Original) The system according to claim 29, wherein said at least one receiver is adapted to establish at least one virtual channel between said originating access device and a terminating access device.

41. (Original) The system according to claim 40, wherein said at least one receiver is adapted to tunnel information between said originating access device and said terminating access device.

42. (Previously presented) The system according to claim 40, wherein said at least one receiver is adapted to establish at least a portion of said at least one virtual channel over at least a portion of one of said first PHY channel, said second PHY channel or said third PHY channel.